BARRACK RODOS & BACINE
STEPHEN R. BASSER (121590)
sbasser@barrack.com
SAMUEL M. WARD (216562)
sward@barrack.com
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

GOLDMAN SCARLATO & PENNY, P.C.
MARK S. GOLDMAN
goldman@lawgsp.com
8 Tower Bridge, Suite 1025
161 Washington Street
Conshohocken, PA 19428
Telephone: (484) 342-0700
Facsimile: (484) 580-7406

Attorneys for Plaintiff Shawn Crane

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

SHAWN CRANE,	Case No.:
Plaintiff,	CLASS ACTION
vs.	
ANTHEM, INC.	CLASS ACTION COMPLAINT
Defendant.	DEMAND FOR JURY TRIAL

Plaintiff Shawn Crane ("Plaintiff"), individually, and on behalf of the Class defined below of similarly situated persons, files this Class Action Complaint, against Anthem, Inc. ("Anthem").

I. INTRODUCTION

1. In 2014 and 2015, Anthem experienced one of the largest data security breaches in history (the "Anthem Data Breach"). Cyberattackers stole the personal information of approximately 80 million Americans ("Affected Individuals").

2. Despite the fact that it was storing sensitive personal information that it knew was valuable to, and vulnerable to, cyberattackers, Anthem failed to take even the most basic security precautions that could have protected Affected Individuals' data. Instead, Anthem used grossly inadequate computer systems and data security practices that allowed the hackers to easily make off with Affected Individuals' personal data. Stealing this much data takes time, and there were numerous steps along the way when any company following standard IT security practices would have foiled the hackers. But Anthem failed to take these basic precautions.

3. Anthem placed the personal information of approximately 80 million Americans in one centralized database (the "Anthem Database"). The Anthem Database included the types of information that federal and state law requires companies to take security measures to protect: names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, employment information, income data, and confidential medical records ("Personal Information"). These data should have received extra protection, not substandard protection.

4. Defendant made repeated promises and representation s to Affected Individuals, by mail and on its website, that they were protecting this sensitive information. Defendant promised that it would provide reasonable security in accordance with federal and state law. It did not.

5. Having done the cyberattackers the favor of compiling the highly sensitive information of 80 million individuals in one place, Defendant failed to implement basic industry-accepted data security tools to prevent cyberattackers from accessing the Anthem Database: Defendant did not require the users of its computer systems to use a two-factor authentication procedure to enter its computer systems; Defendant did not require users to change their passwords; and Defendant allowed users to access personal information even when those users did not need to access that information for job-related purposes. Defendant also failed to encrypt the sensitive personal information within the Anthem Database. If Defendant had taken even one of these basic security steps, the cyberattackers would not have been able to access or use Affected Individuals' sensitive personal information.

6. Any company with reasonable data security practices and procedures – especially one guarding valuable data that were a known target for cyberattackers – would monitor for a data security breach. In other words, even if a company negligently left the "bank vault" open (as Defendant did), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. However, Defendant failed to implement (or turned off) many standard monitoring and alerting systems. Defendant did have some monitoring systems turned on, and those systems sent out alerts when the cyberattackers entered various parts of Defendant's computer systems and when the cyberattackers stole valuable personal information from the Anthem Database. Defendant either failed to review many of these alerts, or ignored the alerts. As time went on, the cyberattackers were stealing so much data (i.e., highly sensitive personal information) that basic information technology maintenance systems should have recognized and stopped the attack. Unfortunately, Defendant failed to properly implement those systems as well.

7. Since the Anthem Data Breach, Affected Individuals have been repeatedly harmed. For example, Affected Individuals have had fake tax returns filed in their names, allowing criminals to abscond with their tax refunds, have had bank accounts drained, and have had credit cards or fraudulent loans taken out in their names. They have spent countless hours

filing police reports and poring over credit reports to combat identity theft, but new fraud is still being perpetrated against them using the sensitive information taken during the Anthem Data Breach. Many are now paying monthly or annual fees for identity theft and credit monitoring services. Now that their sensitive personal information (e.g., their Social Security numbers, dates of birth, and home addresses) has been released, Affected Individuals must worry about being victimized throughout the rest of their lives.

8. Because Defendant failed to provide even minimally adequate computer systems and data security practices, Affected Individuals are forced to suffer the consequences. This Court must hold Defendant accountable.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in each of the proposed class, and at least one member of the class of Plaintiff is a citizen of a state different from a Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant conducts business in the state of California.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. INTRADISTRICT ASSIGNMENT

12. Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Jose Division of the Northern District of California (the "Division") is proper, because a substantial part of the events or omissions which give rise to the claims occurred in this Division. Defendant sells health insurance plans in this Division, maintain offices in this Division, employ workers in this

Division, and advertises in this Division. Assignment to the San Jose Division is also proper because cases relating to the Anthem data breach have been centralized before the Honorable Lucy Koh by the Judicial Panel on Multidistrict Litigation as In re Anthem, Inc. Customer Data Breach Security Litig., No. 5:15-md-02617-LHK (N.D. Cal.)

IV. PARTIES

A. Plaintiff

13. Plaintiff Shawn Crane ("Mr. Crane") is a citizen and resident of the State of Montana. Mr. Crane was enrolled in an Anthem health plan and paid premiums on a regular basis. Anthem and Anthem Blue Cross and Blue Shield collected and received Mr. Crane's Personal Information, which Anthem maintained in its database. Mr. Crane received a letter from Anthem informing him that his Personal Information may have been compromised as a result of the Anthem Data Breach. Mr. Crane now engages in monthly monitoring of his credit and his bank accounts. As a result of the Anthem breach, Mr. Crane has spent numerous hours addressing issues arising from the Anthem Data Breach.

B. Defendant

14. Defendant Anthem, Inc. ("Anthem") is incorporated and headquartered in Indiana. Anthem is one of the largest health benefits and health insurance companies in the United States. Anthem serves its medical members through its health benefits and insurance subsidiaries and affiliates ("Anthem Affiliates"). Anthem is the parent company of the Anthem Affiliates. Anthem also cooperated with other independent Blue Cross Blue Shield licensee insurance and health benefit companies ("non-Anthem BCBS") to create the BlueCard program.

IV. STATEMENT OF FACTS

A. The Anthem Database

15. Anthem is one of the largest health benefits and health insurance companies in the United States. Anthem serves its medical members through its fourteen Blue Cross Blue Shield ("BCBS") licensee affiliates ("Anthem BCBS Affiliates"), as well as its non-Blue Cross Blue Shield affiliates ("Anthem non-BCBS Affiliates"), such as Amerigroup Corporation, CareMore Health Group, Inc., HealthLink, and UniCare. (Collectively, Anthem's health benefits and insurance subsidiaries and affiliates will be referred to as "Anthem Affiliates.")

16. Anthem also cooperated with other independent Blue Cross Blue Shield licensee insurance and health benefit companies ("non-Anthem BCBS") to create the BlueCard program. Under the BlueCard program, members of one BCBS licensee may access another BCBS licensee's provider networks and discounts when the members are out of state. Thus, non-Anthem BCBS members may access an Anthem BCBS Affiliate's provider discounts and network when they travel to an area where an Anthem Affiliate serves as the BCBS licensee.

17. As health insurance and health benefits companies, Anthem, Anthem Affiliates, and non-Anthem BCBS collect, receive, and access its customers' and members' extensive individually identifiable health record information. These records include personal information (such as names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data) and individually-identifiable health information (pertaining to the individual claims process, medical history, diagnosis codes, payment and billing records, test records, dates of service, and all other health information that an insurance company has or needs to have to process claims). (Collectively, both the personal information and individually identifiable health information will be referred to as "Personal Information.")

18. Anthem created a common computer database that it referred to as a "single data warehouse" and the "main subscriber file" containing Personal Information for tens of millions of individuals (the "Anthem Database"). The Anthem Database includes Personal Information

that was provided by current and former customers or members of Anthem Affiliates.. The Anthem Database also includes Personal Information for current and former customers or members of non-Anthem BCBS plans who obtained health care services in areas where Anthem Affiliates serve as the BCBS licensees, as well as employees of self-insured employer groups where Anthem received information about non-Anthem members to provide analytics and administrative services. The Anthem Database also contains Personal Information for Anthem and Anthem Affiliate employees.

19. Anthem publicly admitted that the Anthem Database contained information from former customers or members going back to 2004, and that Anthem generally retains data for 10 years, even though Anthem acknowledges it is not legally required to retain data going back that far in time.

20. Further discovery may demonstrate that the Anthem Database contained information regarding additional individuals.

B. Defendant Promised to Protect Personal Information

21. At all times relevant to this litigation, Anthem and its Affiliates, including Anthem Blue Cross and Blue Shield, have had privacy policies committing to maintain and protect the confidentiality of information that Anthem and its Affiliates collected from their customers in the course of doing business, including personal and health-related information.

22. At all times relevant to this litigation, Anthem's and its Affiliates' privacy policies included a "Personal Information (Including Social Security Number) Privacy Protection Policy" that applied to all members with whom Anthem does business. Since at least 2010 (and on information and belief for many years prior to that), that Policy has stated the following:

> **Anthem Blue Cross and Blue Shield maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members and associates in the course of its regular business functions. Anthem Blue Cross and Blue Shield is committed to**

protecting information about its customers and associates, especially the confidential nature of their personal information (PI). [1]

Personal Information is information that is capable of being associated with an individual through one or more identifiers including but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

- **Anthem Blue Cross and Blue Shield is committed to protecting the confidentiality of Social Security numbers and other Personal Information.**
- **Anthem Blue Cross and Blue Shield's Privacy Policy imposes a number of standards to:**
    - **guard the confidentiality of Social Security numbers and other personal information,**
    - **prohibit the unlawful disclosure of Social Security numbers, and**
    - **limit access to Social Security numbers.**

Anthem Blue Cross and Blue Shield will not use or share Social Security numbers or personal information with anyone outside the company except when permitted or required by federal and state law.

[1] In some of their materials, Defendant utilized the term "Personal Health Information" ("PHI") to refer to health information and "Personally Identifiable Information" ("PII" or "PI") to refer to non-health individually identifiable information.

Anthem Blue Cross and Blue Shield Associates must only access Social Security numbers or personal information as required by their job duties. Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law.

Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

If you have questions regarding this policy, please contact Customer Service by dialing the number that is located on the back of your ID card.

(Emphasis added). The exact language of this Policy has not changed since 2010, and on information and belief, for many years prior to that.

C. Defendant Had an Obligation to Protect Personal Information under Federal and State Law and the Applicable Standard of Care

23. Defendant is an entity covered by HIPAA (see 54 C.F.R. §160.102) and as such are required to comply with HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

24. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[2] In response to the Anthem Data Breach, a senior Department of Health and Human Services advisor explained that "[t]he personally identifiable information health plans maintain on enrollees and members –

[2] 45 C.F.R. §164.502 (2009).

including names and social security numbers – is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed."[3]

25. HIPAA requires that Defendant implement appropriate safeguards for this information.[4]

26. HIPPA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.[5]

27. Additional, HIPPA requires that Defendant:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);

(b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);

(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);

(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, see 45 C.F.R. § 164.306(a)(3);

(e) Ensure compliance with the HIPAA security standard rules by its workforce, see 45 C.F.R. § 164.306(a)(4); and

---

[3] Elizabeth Weise, *Anthem fined $1.7 million in 2010 breach,* USA TODAY (Feb. 5, 2015, 6:13 PM), (http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345.

[4] 45 C.F.R. § 164.530(c)(1)(2009).

[5] 45 C.F.R. § 164.404 (2009); 45 C.F.R. § 164.402 (2009).

(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

28. Defendant is also an entity covered by Gramm-Leach-Bliley, 15 U.S.C. § 6801, *et. seq*. Thus, Defendant had an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801.

29. Defendant is prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act.[6]

30. As described below, Defendant is also required by various state laws and regulations to protect individuals' Personal Information.

31. In addition to its obligations under federal and state laws, Defendant owed a duty to Affected Individuals, who entrusted them with sensitive Personal Information, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Affected Individuals to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of the Affected Individuals.

32. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to design, maintain, and test its computer systems to ensure that the Personal Information in Defendant's possession was adequately secured and protected.

---

[6] *See e.g., FTC v. Wyndham Worldwide Corp.*, 599 F.3d 236, 243 (3d Cir. 2015).

33. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal Information.

34. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to implement processes that would detect a breach of its data security systems in a timely manner.

35. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to act upon data security warnings and alerts in a timely fashion.

36. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendant, or to entrust Personal Information with Defendant.

37. Defendant owed a duty to Affected Individuals, who entrusted it with sensitive Personal Information, to disclose in a timely and accurate manner when data breaches occurred.

38. Defendant owed a duty of care to Affected Individuals because they were foreseeable and probable victims of any inadequate data security practices. Anthem collected Affected Individuals' Personal Information either directly or indirectly from Anthem Affiliates and/or Non-Anthem BCBS. Anthem knew that a breach of its data systems would cause Affected Individuals to incur damages.

D. Defendant Was On Notice of Cyber Attack Threats, and the Inadequacy of Its Data Security

39. Defendant knew or should have known that Anthem and Anthem Affiliates had previous problems with its data security.

40. In late 2009 and early 2010, over 600,000 customers of Wellpoint (Anthem's former trade name) and Blue Cross of California had their personal information and protected healthcare information compromised due to a data breach. Customers' Personal Information had not been password protected.[7]

41. In 2013, the Department of Health and Human Services fined Anthem $1.7 million for HIPAA violations. The HHS' Office for Civil Rights found that Anthem "had not enacted appropriate administrative, technical, and physical safeguards for data as required by HIPAA.[8]

42. Also in 2013, the OIG conducted an audit of Wellpoint's information system pursuant to the Federal BCBSA Contract. In September 10, 2013, the OIG issued a report titled "Audit of Information System General and Applications Controls at Wellpoint, Inc." The purpose of the audit was to examine the "information systems used to process BCBSA's [insurance claims], as well as the various business processes and IT systems used to support these applications."

43. One of the tests OIG routinely conducts is a configuration compliance audit, which is the process of routinely comparing the actual security configuration of computer servers to an approved baseline configuration. In its audit report, OIG noted that "[f]ailure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers remain undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches." Despite the importance of ensuring

---

[7] Settlement Agreement, *Blue Cross of California Website Security Cases*, Case No. JCCP 4647 (April 18, 2011 Cal. Super. Ct.), https://anthembluecrosssecuritysettlement.com/SettlementAgreement.pdf.

[8] Rachel Landen and Joseph Conn, *WellPoint to pay $1.7 million HIPAA penalty*, MODERN HEALTHCARE (July 11, 2013), http://www.modernhealthcare.com/article/20130711/NEWS/307119954 (last visited Oct. 19, 2015).

the sufficiency of its configuration compliance auditing program, Wellpoint frustrated OIG's efforts to perform this test, claiming that company policy prohibited external entities such as OIG from accessing Wellpoint's network. As a result, the Federal BCBSA Plan "was unable to provide satisfactory evidence to confirm that it had a program in place to routinely monitor the configuration of its servers." After the Anthem Data Breach, Anthem again refused to submit itself to standard tests for determining the vulnerability of its computer systems, again citing "corporate policy."

44. Despite Wellpoint's efforts to frustrate the OIG audit, OIG was able to determine that Wellpoint's information systems were deficient in at least the following ways: (i) weaknesses in privileged user monitoring, (ii) no implementation of controls to prevent rogue devices from accessing the network, (iii) not subjecting all servers to routine vulnerability scans, and (iv) Wellpoint's mainframe password settings were not in compliance with its own standards. OIG offered numerous recommendations for how Wellpoint could improve its data security procedures. On information and belief, Wellpoint failed to implement all or many of OIG's recommendations.

45. Defendant was also on notice that healthcare companies were targets for cyberattacks. Indeed, Anthem publicly admitted that Anthem itself is subject to several hundred credible hacking threats per month.

46. Defendant was on notice that the FBI was concerned about healthcare company data security. In August 2014, after a cyber-attack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them.[9] The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

---

[9] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014, 4:32 PM), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GH24U20140820.

47. Defendant was on notice that the federal government was concerned about healthcare company data encryption and Anthem knew a large portion of the Anthem Database was not encrypted. The United States Department of Health and Human Services' Office for Civil Rights urges health care providers and insurers to encrypt data containing sensitive personal information. In April 2014, the Department fined Concentra Health Services and QCA Health Plan Inc. of Arkansas approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS' Office of Human Rights' deputy director of health information privacy, stated "[our] message to these organizations is simple: encryption is your best defense against these incidents."

48. Defendant was also on notice of the threat of cyberattacks due to prior, high-profile security breaches at retail chains such as Home Depot, Target, and Neiman Marcus, as well as the hundreds of credible cyber threats that Anthem received on a monthly basis.

E. Anthem Allowed A Massive Data Breach

49. In February, 2015, after it began to receive media inquiries, Anthem announced to the general public that cyberattackers had breached the Anthem Database, and accessed Personal Information about individuals in the Anthem Database.[10]

50. Anthem later announced that the hackers had accessed Personal Information for 78.8 million people.[11]

51. Anthem admits that the information accessed about Affected Individuals included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data.[12]

---

[10] https://www.anthemfacts.com/ (last visited Oct. 19, 2015)

[11] Anna Mathews, *Anthem: Hacked Database Included 78.8 Million People*, WALL STREET JOURNAL (Feb. 24, 2015, 2:49 PM), http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.

[12] https://anthemfacts.com/ (last visited Oct. 19, 2015).

52. On information and belief, medical and health care information was also stolen from Affected Individuals during or as a result of the Anthem Data Breach. On information and belief, the data that Anthem admits were compromised, including Social Security Numbers and dates of birth, can be used to access medical and health care information through Anthem, Anthem affiliates, and non-Anthem BCBS' online portals. News reports corroborate that medical data were stolen from Affected Individuals during the Anthem Data Breach.

53. Anthem and Anthem Affiliates' computer systems and data security practices were grossly inadequate to secure the highly sensitive and valuable Personal Information that had been entrusted to them. Anthem and Anthem Affiliates' failures were widespread.

54. First, Anthem and Anthem Affiliates failed to implement basic industry-accepted data security tools to prevent cyberattackers from accessing the Anthem Database: (i) Anthem and Anthem Affiliates did not implement a two-factor authentication procedure for users to enter its computer system, instead allowing users to access the Anthem Database from external computers using only a single password. (Conversely, in a two-factor authentication system, a user first enters his or her password, and then the user is sent a one-time second password (the second factor) to a personal device. The user receives a different second password every time that the user signs on to his or her account.) Two-factor authentication has been a security best practice for remotely accessible systems for decades, and its importance is widely known by Information Technology professionals. (ii) Anthem and Anthem Affiliates did not require users to change their passwords on a regular basis, and allowed some users to keep the same password for years. (iii) Anthem and Anthem Affiliates allowed Anthem employees to access Personal Information even when those users did not need to access that information for job-related purposes. If Anthem had implemented any of these basic data security tools, the cyberattackers would not have been able to access Affected Individuals' Personal Information, or would not have been able to access so much of Affected Individuals' Personal Information.

55. Second, Anthem and Anthem Affiliates failed to implement basic policies and procedures that could have prevented the attack. For example, Anthem failed to train employees to identify, report, and delete "phishing" email.

56. Third, Anthem and Anthem Affiliates failed to implement monitoring and alerting that would have alerted them to the cyberattack during the many months and years that the attack was ongoing. Anthem and Anthem Affiliates failed to even implement simple Information Technology maintenance systems that would have discovered the cyberattackers. Even if the cyberattackers gained access to the Anthem Database, Anthem could have and should have, but failed to, discover the data breach before any data were exfiltrated.

57. Fourth, even when Anthem and Anthem Affiliates did implement monitoring and alerting systems, on information and belief, they simply ignored the alerts. If Anthem and Anthem Affiliates had taken proper steps once systems alerts were triggered, they could have averted the Anthem Data Breach.

58. Fifth, Anthem and Anthem Affiliates lacked reasonable encryption policies. Anthem's Information Technology Executive, Stacia Grosso, publicly admitted that a large portion of the Anthem Database was not encrypted. Instead, Anthem and Anthem Affiliates only used encryption when data were being moved around within its information environment and for such things as mobile phones and laptops. Anthem also promised after the Anthem Data Breach that it would investigate encryption best practices and determine whether it should encrypt the Anthem Database.

59. On information and belief, Anthem and Anthem Affiliates not only failed to generally encrypt the Anthem Database, they failed to implement specific encryption for sensitive Personal Information within the Anthem Database. Standard industry practice is to encrypt sensitive Personal Information, such as Social Security Numbers. If Anthem had encrypted the sensitive Personal Information within the Anthem Database, even if cyberattackers accessed the Anthem Database, the cyberattackers would have been unable to use the Affected Individuals' Personal Information.

60. The cyberattackers stole Personal Information for approximately 79 million Affected Individuals. On information and belief, Anthem and Anthem Affiliates have still not implemented necessary computer systems and date security practices to ensure that Affected Individuals' Personal Information will not be accessed or stolen by additional cyberattackers. The remediation measures implemented by Anthem and Anthem Affiliates provided only an immediate stop to the present attack and did not indicate that Anthem and Anthem Affiliates had made any changes to the policies, procedures, management methods, or practices which allowed these attacks to occur in the first place. Each day, new individuals' Personal Information is entered into the Anthem Database, and this Personal Information is at risk until Anthem and Anthem Affiliates improve their data security. Anthem and Anthem Affiliates must put into place a security management framework, as defined by numerous government standards, and conduct audits by third-party independent auditors on a regular basis, to ensure that it keeps abreast of future threats to the Personal Information in its care.

F. Anthem's Data Breach Was a Direct Result of Anthem's Inadequate Data Security

61. Affected Individuals' Personal Information was compromised in the Anthem Data Breach because Defendant violated its promises and legal obligations to maintain the security of the highly sensitive Personal Information that Affected Individuals entrusted to Defendant.

62. Despite its promises and legal obligations, Defendant did not provide reasonable or adequate security for Affected Individuals' Personal Information. As the creator and main operator of the Anthem Database, Anthem is responsible for the inadequate and unreasonable computer systems and data security practices as well as the unnecessarily large amount of unneeded data contained in that database.

63. Defendant breached its duties to Affected Individuals by the conduct alleged in the Complaint.

64. Defendant breached its duty to Affected Individuals to design, maintain, and test its computer systems to ensure that Affected Individuals' Personal Information was adequately secured in many ways, including, but not limited to:

(a) failing to create a two-factor-authentication system for users;

(b) failing to encrypt the Anthem Database or the sensitive Personal Information within the Anthem Database;

(c) failing to require users to create new passwords within a limited time period, such as 90 days;

(d) failing to restrict access to sensitive Personal Information within the Anthem Database to users who had a job-related reason to be accessing that particular Personal Information;

(e) failing to turn on all of the logging functions on all its computer systems;

(f) failing to aggregate and monitor logging functions;

(g) failing to implement internal proper access controls for Personal Information, allowing users to access Personal Information even though they did not have job functions that required them to access Personal Information; and

(h) failing to adequately update its computer systems even though those systems had been demonstrated to be inadequate by 2014 because of previous security breaches.

65. 66. Defendant breached its duty to Affected Individuals to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession in many ways, including, but not limited to:

(a) failing to respond to all system alerts;

(b) continuing to use social security numbers (SSNs) to identify members even though other health insurance companies switched to unique member identification numbers (MINS) as early as 2003;

(c) failing to adequately train all users of the Anthem Database on data security practices;

(d) needlessly maintaining information regarding former customers (as far back to 2004) on its databases and servers[13]. Had Defendant simply put inactive members' information on backup servers or tapes, the scope of the breach would have been smaller;

(e) failing to adequately train users of Anthem and Anthem Affiliates' computer system on how to identify spear-fishing e-mail;

(f) failing to provide a framework for escalation of suspicious events; and

(g) failing to adequately update its data security practices and procedures even though those practices and procedures had been demonstrated to be inadequate by 2014 because of previous security breaches.

66. Defendant breached its duty to Affected Individuals to implement processes that would detect a breach of its data security systems in a timely manner in many ways, including, but not limited to:

(a) failing to aggregate, filter, and report on log and alert information in a unified manner,

(b) failing to turn on all of the "logging" function on its computer systems,

(c) failing to implement a reasonable capacity monitoring and alerting system; and

(d) failing to implement basic Information Technology monitoring systems that would have detected the cyberattackers' activities, such as monitoring data usage on the system, monitoring data extraction, or performance monitoring.

67. Defendant breached its duty to Affected Individuals to act upon data security warnings and alerts in a timely fashion by:

(a) failing to respond to multiple alerts of cyberattacker activity, including a month-long alert;

---

[13] *See, e.g.,* Anthem Data Breach, Cal. Dept. of Ins., http://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm (last visited Oct. 19, 2015).

(b) failing to aggregate, filter, and report on log and alert information in a unified manner,

(c) failing to periodically review alert information; and

(d) failing to periodically review log information.

68. Defendant breached its duty to Affected Individuals to disclose the material fact that Anthem and Anthem Affiliates' computer systems and data security practices were inadequate to safeguard Affected Individuals' Personal Information. Had Defendant disclosed to Affected Individuals that its computer systems and data security practices were inadequate to safeguard Affected Individuals' highly sensitive Personal Information, Affected Individuals would not have entrusted their Personal Information to Defendant and would not have enrolled in its insurance or health care plans.

69. Anthem and Anthem Affiliates breached their duty to Affected Individuals to disclose in a timely and accurate manner that the Anthem Data breach had occurred. Anthem and Anthem Affiliates failed to notify potentially affected customers for several weeks, and in some cases months, after they claim they discovered the breach. Indeed, several states joined together to write to Anthem to urge it to notify Affected Individuals in a more timely manner.[14] As a result, the Affected Individuals were not notified of the Anthem Data Breach until in or about March 2015. Additionally, further discovery will be needed to determine whether Anthem and Anthem Affiliates discovered the breach earlier.[15]

---

[14] Jim Finkle, *U.S. states say Anthem too slow to inform customers of breach*, REUTERS, (Feb. 11, 2015, 11:18 AM), http://www.reuters.com/article/2015/02/11/us-anthem-cybersecurity-states-idUSKBN0LE2QP20150211.

[15] There are reports that Anthem's website dedicated to the security breach – www.anthemfacts.com – was registered on December 13, 2014. *See e.g.*, Dan Goodin, *String of big data breaches continues with hack on health insurer Anthem*, ARSTECHNICA (Feb. 5, 2015, 11:01 AM), http://arstechnica.com/security/2015/02/string-of-big-data-breaches-continues-with-hack-on-health-insurer-anthem./ (accessed Feb. 8, 2015).

70. Anthem and Anthem Affiliates' failure to notify Affected Individuals of the Anthem Data Breach in a timely and accurate manner allowed the cyberattackers to begin to use Affected Individuals' Personal Information before Affected Individuals had an opportunity to take steps to protect themselves. For example, many Affected Individuals had fraudulent 2015 tax returns filed in their names. While Anthem and Anthem Affiliates became aware of the Anthem Data Breach near the beginning of the federal tax filing period, they failed to notify the Affected Individuals until near the end of the federal tax filing period. This deprived Affected Individuals of the opportunity to take steps to avoid fraudulent tax filings.

71. Defendant violated its promises and representations contained in its mailed privacy notices and website privacy statements.

72. Defendant violated its promises by failing to adequately maintain "policies that protect the confidentiality of personal information, including Social Security numbers."

73. Defendant violated its promises by failing to impose "a number of standards to: guard the confidentiality of Social Security numbers and other personal information, prohibit unlawful disclosure of Social Security numbers, and limit access to Social Security numbers."

74. Defendant violated its promise to comply with federal and state law to maintain the security of Affected Individuals' Personal Information, such as HIPAA. For example, Defendant violated HIPAA by failing to establish procedures to keep the Personal Information in its possession confidential and private.

75. Defendant violated the Gramm-Leach-Bliley Act by failing to protect the security and confidentiality of those customers' "nonpublic personal information." 15 U.S.C. § 6801.

76. Defendant violated the Federal Trade Commission Act by engaging in the "unfair practice" of failing to maintain reasonable and appropriate data security for consumers' sensitive Personal Information.

G. Affected Individuals Were Grievously Harmed By the Anthem Data Breach

77. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

78. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[18]

79. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit various types of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

80. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

[16] 17 C.F.R. §248.201 (2013).

[17] *Id.*

[18] *Guide for Assisting Identity Theft Victims,* Federal Trade Commission, 4 (September 2013), http://www.consumer .ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Oct. 19, 2015).

81. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[19]

82. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

83. The injuries suffered by the Affected Individuals are a direct and proximate result of the Anthem Data Breach and include:

(a) theft of their personal and financial information;

(b) loss or delay of tax refunds as a result of fraudulently filed tax returns;

(c) costs associated with the detection and prevention of identity theft and unauthorized use of their Personal Information and financial, business, banking, and other accounts;

(d) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Anthem Data Breach, including finding fraudulent charges, cancelling credit cards, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Anthem Data Breach, including additional phishing emails and phone scams;

(e) the imminent and certain impending injury flowing from fraud and identify theft posed by their Personal Information being placed in the hands of hackers;

---

[19] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), http://news.cnet.com/8301-27080_3-10460902-245.html.

(f) damages to and diminution in value of their Personal Information entrusted to Defendant for the sole purpose of obtaining health insurance or health care services from Anthem, Anthem Affiliates (including BCBS) and Non-Anthem BCBS and with the mutual understanding that Defendant would safeguard Affected Individuals' data against theft and not allow access to or misuse of their data by third parties;

(g) money paid to Defendant for health insurance or health care services during the period of the Anthem Data Breach because Plaintiff and Class Members would not have obtained health insurance or health care services from Defendant had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Personal Information;

(h) losing the benefit of their bargain that Affected Individuals entered into a bargain for health insurance benefits or health insurance in which Defendant would take reasonable and adequate security measures to protect Affected Individuals' Personal Information, which Defendant failed to do;

(i) damages caused by Defendant's failure to notify Affected Individuals about the Anthem Data Breach in a timely and accurate fashion; and

(j) continued risk to Affected Individuals' Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that Affected Individuals entrusted to Defendant.

84. Anthem itself acknowledges the harm caused by the Anthem Data Breach because it offered Affected Individuals twenty-four months of identity theft repair and credit monitoring services. Two years of identity theft repair and credit monitoring is woefully inadequate to protect Affected Individuals from a virtual lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

85. Anthem publicly stated that any identity theft repair or credit monitoring services potentially offered beyond twenty-four months will be embedded in Anthem's pricing. Anthem

also stated it will not reimburse individuals that purchase identity theft repair or credit monitoring services.[20]

V. CLASS ALLEGATIONS

A. Montana Class

86. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims for negligence (Count I), negligence per se (Count II), negligent misrepresentation (Count III), and unjust enrichment (Count IV), as well as statutory claims under the Montana Unfair Trade Practices and Consumer Protection Act (Count V), and Montana Insurance Information and Privacy Protection Act (Count VI) on behalf of the Montana Class, defined as follows: :

> **Montana Class:** All residents of Montana whose Personal Information was maintained on the Anthem Database and was compromised as a result of the breach announced by Anthem on or around February 5, 2015.

87. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

B. Certification of the Proposed Class is Appropriate

88. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

89. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but there are approximately 48,000 individuals in the Montana Class, making

[20] https://anthemfacts.com/faq

joinder of each individual impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

90. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class' Personal Information;

b) Whether Defendant failed to protect Plaintiff's and the Class' Personal Information, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class' Personal Information violated HIPAA, federal, state and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class' Personal Information properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and state medical privacy statutes applicable to Plaintiff and each Class member;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Anthem Data Breach as soon as practical and without delay after the Anthem Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Personal Information;

h) Whether Defendant entered into contracts with Plaintiff and the members of the each of the Class that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's Personal Information and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of its contracts with Plaintiff and the members of each of the Class;

j) Whether Defendant should retain the money paid by Plaintiff and members of each of the Class to protect their Personal Information;

k) Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the members of the Class are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

91. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

92. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

93. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Anthem

Database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Anthem Database.

94. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

95. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

COUNT I - NEGLIGENCE

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

96. Plaintiff incorporates the above allegations by reference.

97. Defendant required Plaintiff and Montana Class Members to submit Personal Information in order to obtain insurance coverage and/or to receive health care services.

98. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and Montana Class Members.

99. As described above, Anthem owed duties of care to Plaintiff and Montana Class Members whose Personal Information had been entrusted with Anthem. Anthem Blue Cross and Blue Shield owed duties of care to Plaintiff and Montana Class Members whose information was placed in the Anthem Database due to their dealings with Anthem Blue Cross and Blue Shield.

100. Defendant breached its duties to Plaintiff and Montana Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's Personal Information.

101. Defendant acted with wanton disregard for the security of Plaintiff's and Montana Class Members' Personal Information. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the Personal Information in health care databases, such as Anthem's. A "special relationship" exists between Defendant and the Plaintiff and Montana Class Members. Anthem Blue Cross and Blue Shield entered into a "special relationship" with the Plaintiff and Montana Class Members whose Personal Information was requested, collected, and received by Anthem Blue Cross and Blue Shield. Anthem entered into a "special relationship" with Plaintiff and Class Members because Anthem placed their Personal Information in the Anthem Database – information that

Plaintiff and State Class Members had been required to provide to Anthem Blue Cross and Blue Shield.

102. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Montana Class Members, Plaintiff and Montana Class Members would not have been injured.

103. The injury and harm suffered by Plaintiff and Montana Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet its duties, and that Defendant's breach would cause Plaintiff and Montana Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

104. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II - NEGLIGENCE PER SE

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

105. Plaintiff incorporates the above allegations by reference.

106. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

107. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Personal Information.

108. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Personal Information.

109. Defendant breached its duties to Plaintiff and Montana Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), and

Gramm-Leach-Bliley Act (15 U.S.C. § 6801) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information and by failing to promptly notify Plaintiff and Class Members of the breach.

110. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

111. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Montana Class Members, Plaintiff and Montana Class Members would not have been injured.

112. The injury and harm suffered by Plaintiff and Montana Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Montana Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

113. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III - NEGLIGENT MISREPRESENTATION

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

134. Plaintiff incorporates the above allegations by reference.

135. Defendant negligently and recklessly misrepresented material facts, pertaining to the sale of insurance and health benefits services, to Plaintiff and Montana Class Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Montana Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft.

136. Defendant negligently and recklessly misrepresented material facts, pertaining to the sale of insurance and health benefits services, to Plaintiff and Montana Class Members by

representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff and Montana Class Members' Personal Information.

137. Because of multiple warnings about the inadequacy of its data privacy and security practices, Defendant either knew or should have known that its representations were not true.

138. In reliance upon these misrepresentations, Plaintiff and Montana Class Members purchased insurance or health benefits services from Defendant.

139. Had Plaintiff and Montana Class Members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Personal Information, they would not have purchased insurance or health benefits services from Defendant, and would not have entrusted their Personal Information to Defendant.

140. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT IV - UNJUST ENRICHMENT

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

141. Plaintiff incorporates the above allegations by reference.

142. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of premiums paid for the purchase of health insurance and health benefits services.

143. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

144. The premiums for health insurance and health benefits services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

145. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between health insurance and health benefit services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate health insurance and health benefits services without reasonable data privacy and security practices and procedures that they received.

146. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

147. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant.

148. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

149. Plaintiff and Class Members have no adequate remedy at law.

COUNT V – MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, MCA § 30-14-101, *et. seq.*

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

150. Plaintiffs incorporate the above allegations by reference.

151. Plaintiffs bring this claim against Defendant on behalf of the Montana Class.

152. The Montana Class Members are "consumers" as meant by Mont. Code § 30-14-102.

153. The Montana Class Members purchased insurance and health benefits services from Defendant in "trade" and "commerce," as meant by Mont. Code § 30-14-102, for personal, family, and/or household purposes.

154. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Montana Class in violation Mont. Code § 30-14-103, including but not limited to the following:

a. Defendant misrepresented material facts, pertaining to the sale of insurance and health benefits services, to the Montana Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Montana Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Defendant misrepresented material facts, pertaining to the sale of insurance and health benefits services, to the Montana Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Montana Class Members' Personal Information;

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Montana Class Members' Personal Information;

d. Defendant engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance and health benefits services by failing to maintain the privacy and security of Montana Class Members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Anthem Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, et seq.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the Montana Insurance Information and Privacy Protection Act (Mont. Code Ann. § 33-19-306); and the Montana Unfair Claim Settlement Practices Act (Mont. Code Ann. § 33-18-201(1));

e. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of insurance and health benefits services by failing to disclose the Anthem Data Breach to Montana Class Members in a timely and accurate manner, in violation of Mont. Code Ann.§ 30-14-1704(1);

f. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of insurance and health benefits services by failing to take proper action following the Anthem Data Breach to enact adequate privacy and security measures and protect Montana Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

155. The above unlawful, unfair, and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

156. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Montana Class Members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Montana Class.

157. As a direct and proximate result of Defendant's deceptive acts and practices, the Montana Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

158. Montana Class Members seek relief under Mont. Code § 30-14-133, including, but not limited to, injunctive relief, other equitable relief, actual damages or $500 per Class Member, whichever is greater, treble damages, and attorneys' fees and costs.

COUNT VI – MONTANA INSURANCE INFORMATION AND PRIVACY PROTECTION ACT (MONT. CODE § 33-19-101, *et seq.*)

BROUGHT BY MONTANA CLASS AGAINST ANTHEM

159. Plaintiffs incorporate the above allegations by reference.

160. Plaintiffs bring this claim against Defendant on behalf of the Montana Class whose personal information was compromised as a result of the Anthem Data Breach.

161. Defendant is an "insurance institution" as defined by the Montana Insurance Information and Privacy Protection Act, Mont. Code § 33-19-104.

162. Defendant collected and received "personal information," as defined by the Montana Insurance Information and Privacy Protection Act, Mont. Code § 33-19-104, regarding members of the Montana Class in connection with insurance transactions.

163. Defendant disclosed personal information regarding members of the Montana Class that was collected or received in connection with insurance transactions without Montana Class Members' written authorization, in violation of Mont. Code Ann. § 33-19-306. Upon information and belief, the disclosure of personal information to unauthorized individuals in the Anthem Data resulted from the affirmative actions of Anthem employees. Thus, Anthem actively and affirmatively allowed the cyberattackers to see and obtain individually-identifiable personal information regarding members of the Montana Class.

164. The Anthem Data Breach compromised Personal Information and violated the rights of members of the Montana Class

165. The Montana Class suffered injury from Defendant's illegal disclosure and failure to maintain the confidentiality of their personal information.

166. The Montana Class seeks relief under Mont. Code Ann. § 33-19-407 including but not limited to actual damages, nominal damages, injunctive relief, and/or attorneys' fees and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Montana Class, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointed the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein.

B. Plaintiff requests injunctive relief. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test its computer systems to ensure that Personal Information in its possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendant to implement multi-factor authentication requirements; (viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Defendant to encrypt all Personal Information; (x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Anthem to segment data by, among other things, creating firewalls and access controls so that if one area of the Anthem network is compromised, hackers cannot gain access to other portions of Anthem's systems; (xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for its provision of services; (xiii) requiring Defendant to conduct regular database scanning and securing checks; (xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel

how to identify and contain a breach when it occurs and what to do in response to a breach; (xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to members of the Class; and (xvi) requiring Defendant to educate all class members about the threats they face as a result of the loss of their Personal Information to third parties, as well as steps Class Members must take to protect themselves.

C. Plaintiff also requests actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement of profits, attorney's fees, statutory costs, and such other and further relief as is just and proper. Plaintiff seeks attorneys' fees under California Code of Civil Procedure 1021.5, and similar statutes under other state laws.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: April 11, 2016

Respectfully submitted,

Stephen R. Basser (121590)
Samuel M. Ward (216562)
BARRACK, RODOS & BACINE

/s/ STEPHEN R. BASSER
STEPHEN R. BASSER

600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

MARK S. GOLDMAN
goldman@lawgsp.com
GOLDMAN SCARLATO & PENNY, P.C.
8 Tower Bridge, Suite 1025
161 Washington Street
Conshohocken, PA 19428
Telephone: (484) 342-0700
Facsimile: (484) 580-8747

Attorneys for Plaintiff Shawn Crane